

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-82610  
(P2002-82610A)

(43) 公開日 平成14年3月22日 (2002. 3. 22)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 C 0 5 9
H 0 4 N 1/387		H 0 4 N 1/387	5 C 0 6 3
7/08		7/08	Z 5 C 0 7 6
7/081		7/13	Z 5 J 1 0 4
7/24			

審査請求 未請求 請求項の数24 O L (全 15 頁)

(21) 出願番号 特願2000-270409(P2000-270409)

(22) 出願日 平成12年9月6日(2000. 9. 6)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 若尾 聡

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

(72) 発明者 田頭 信博

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

(74) 代理人 100090538

弁理士 西山 恵三 (外1名)

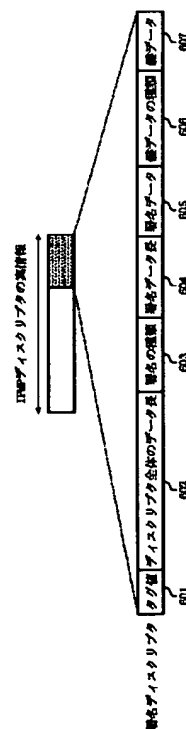
最終頁に続く

(54) 【発明の名称】 コンテンツ作成方法及び装置、コンテンツ再生方法及び装置、並びにコンピュータ可読記憶媒体

(57) 【要約】

【課題】 知的財産保護管理システムを備えるマルチメディア符号化方式において、コンテンツの知的財産権（著作権）に対する保護・管理機能を向上させる。

【解決手段】 コンテンツの送信装置は、MPEG-4等、知的財産保護及び管理のためのIPMPディスクリプタを含むマルチメディアデータを作成する。このとき、IPMPディスクリプタに、コンテンツ内の情報に対して改竄されたか否かを検証するための署名ディスクリプタを埋め込む。



【特許請求の範囲】

【請求項1】 知的財産保護管理システムを備えるマルチメディア符号化方式のコンテンツ作成方法であって、コンテンツ内の情報のオリジナル性を検証するための検証用データを含む知的財産保護管理情報を発生し、前記知的財産保護管理情報をコンテンツに、前記知的財産保護管理システムが使用するメッセージ形態にして埋め込むことを特徴とするコンテンツ作成方法。

【請求項2】 前記検証用データは、情報が改竄されているか否かを検証するためのデータであることを特徴とする請求項1に記載のコンテンツ作成方法。

【請求項3】 前記検証用データは、知的財産保護管理情報が改竄されているか否かを検証するためのデータであることを特徴する請求項2に記載のコンテンツ作成方法。

【請求項4】 前記検証用データは、検証用データが開始されることを表すコードと、前記検証用データのデータ長と、検証のための実データとを少なくとも含むことを特徴とする請求項1～3の何れか1項に記載のコンテンツ作成方法。

【請求項5】 前記マルチメディア符号化方式は、MPEG-4符号化方式であり、前記知的財産保護管理情報は、IPMPストリームであることを特徴とする請求項1～4の何れか1項に記載のコンテンツ作成方法。

【請求項6】 前記マルチメディア符号化方式は、オブジェクト単位で符号化する方式であることを特徴とする請求項1～5のいずれか1項に記載のコンテンツ作成方法。

【請求項7】 前記オブジェクトは、映像情報を有することを特徴とする請求項6に記載のコンテンツ作成方法。

【請求項8】 前記オブジェクトは、音声情報を有することを特徴とする請求項6又は請求項7に記載のコンテンツ作成方法。

【請求項9】 前記知的財産保護管理システムは、コンテンツの著作権を保護管理することを特徴とする請求項1～8の何れか1項に記載のコンテンツ作成方法。

【請求項10】 前記知的財産保護管理システムは、コンテンツの再生制限を行うことを特徴とする請求項1～9の何れか1項に記載のコンテンツ作成方法。

【請求項11】 請求項1～10の何れか1項に記載されたコンテンツ作成方法を実行するためのプログラムを記憶したことを特徴とするコンピュータ可読記憶媒体。

【請求項12】 知的財産保護管理システムを備えるマルチメディア符号化方式のコンテンツ作成装置であって、コンテンツ内の情報のオリジナル性を検証するための検証用データを含む知的財産保護管理情報を発生する発生手段と、前記知的財産保護管理情報をコンテンツに、前記知的財産保護管理システムが使用するメッセージ形態にして埋め込む多重化手段とを有することを特徴

とするコンテンツ作成装置。

【請求項13】 知的財産保護管理システムを備えるマルチメディア符号化方式のコンテンツ再生方法であって、コンテンツ内の情報のオリジナル性を検証するための検証用データを含む知的財産保護管理情報が埋め込まれたコンテンツを入力する入力工程と、前記コンテンツ内の知的財産保護管理情報を検出する検出工程と、前記検出結果に基づいて前記コンテンツの再生動作を制御する制御工程とを有することを特徴とするコンテンツ再生方法。

【請求項14】 前記検証用データは、前記コンテンツ内の情報が改竄されているか否かを検証するためのデータであることを特徴とする請求項13に記載のコンテンツ再生方法。

【請求項15】 前記検証用データは、知的財産保護管理情報が改竄されているか否かを検証するためのデータであることを特徴する請求項14に記載のコンテンツ再生方法。

【請求項16】 前記検証用データは、検証用データが開始されることを表すコードと、前記検証用データのデータ長と、検証のための実データとを少なくとも含むことを特徴とする請求項13～15の何れか1項に記載のコンテンツ再生方法。

【請求項17】 前記マルチメディア符号化方式は、MPEG-4符号化方式であり、前記知的財産保護管理情報は、IPMPストリームであることを特徴とする請求項13～16の何れか1項に記載のコンテンツ再生方法。

【請求項18】 前記マルチメディア符号化方式は、オブジェクト単位で符号化する方式であることを特徴とする請求項13～17のいずれか1項に記載のコンテンツ再生方法。

【請求項19】 前記オブジェクトは、映像情報を有することを特徴とする請求項18に記載のコンテンツ再生方法。

【請求項20】 前記オブジェクトは、音声情報を有することを特徴とする請求項18又は請求項19に記載のコンテンツ再生方法。

【請求項21】 前記知的財産保護管理システムは、コンテンツの著作権を保護管理することを特徴とする請求項13～20の何れか1項に記載のコンテンツ再生方法。

【請求項22】 前記検出工程は、前記検証用データを検出し、コンテンツに改竄されているか否かを検出し、前記制御工程は前記検出結果に応じて前記再生工程の再生動作を抑制することを特徴とする請求項14又は請求項15に記載のコンテンツ再生方法。

【請求項23】 請求項13～22の何れか1項に記載されたコンテンツ再生方法を実行するためのプログラムを記憶したことを特徴とするコンピュータ可読記憶媒体。

・【請求項24】 知的財産保護管理システムを備えるマルチメディア符号化方式のコンテンツ再生装置であって、コンテンツ内の情報のオリジナル性を検証するための検証用データを含む知的財産保護管理情報が埋め込まれたコンテンツを入力する入力手段と、前記コンテンツ内の知的財産保護管理情報を検出する検出手段と、前記検出結果に基づいて前記コンテンツの再生動作を制御する制御手段とを有することを特徴とするコンテンツ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、知的財産（例えば著作権）保護管理システムを備えるマルチメディア符号化方式のコンテンツ作成方法／装置、コンテンツ再生方法／装置、並びにコンピュータ可読記憶媒体に関するものである。

【0002】

【従来の技術】近年、動画像や音声などのデータを符号化し、夫々の符号化データをオブジェクトとして扱い、これらの所謂マルチメディアデータを組み合わせて単一のビットストリームとして伝送する手法として、ISO(International Organization for Standardization)にてMPEG-4(Moving Picture Experts Group part 4)が標準化されつつある。

【0003】MPEG-4符号化方式により符号化されたマルチメディアデータを受信する受信側（再生側）においては例えば、音声と動画シーンを関連付けて再生する。このようなMPEG-4システムにおいては、データがオブジェクトとして扱われるという特性のために、受信したビットストリームをオブジェクト毎に1つ1つバラバラにして再編成するといったことを容易に行うことが可能になる。上述したようなMPEG-4のデータストリームにおいては、これまでの一般的なマルチメディアストリームとは異なり、いくつもの動画シーンや動画オブジェクトを単一のストリーム上で独立して送受信する機能を有する。また音声についても同様にいくつものオブジェクトを単一のストリーム上で独立して送受信する機能を有する。

【0004】これらのオブジェクトを合成してあるシーンを合成するための情報としてVRML(Virtual Reality Modeling Language)を修正したシーン記述情報（BIFS : Binary Format For Scenes）が存在する。このBIFSはシーンが2値で記述されているもので、このBIFSに従ってシーンが合成される。

【0005】このような、シーンの合成に必要な個々のオブジェクトは夫々、個別に最適な符号化が行われて送信されることになるので、復号側でも個別に復号され、BIFSの記述に従い、個々のデータの持つ時間軸を再生装置内部の時間軸に同期させてシーンを合成、出力することになる。

【0006】図1は、一般的なMPEG-4再生装置の概略構成を示すブロック図である。図1において、伝送路101は各種ネットワーク、コンピュータバス等のデータの路であり、MPEG-4ストリームが入力されるネットワークである。ここで、伝送路は通信路の意味の他にCD-ROM、DVD-ROM、DVD-RAMといった記録媒体装置と再生装置とのインターフェースも意味する。

【0007】再生装置において、ネットワークや記録媒体装置から配信されたMPEG-4ストリームは、分離部102に入力される。ここでMPEG4ストリームシーン記述情報、動画像オブジェクトデータ、音声オブジェクトデータ、オブジェクトディスクリプタ等に分離された後、それぞれのメモリ部103～106に入力される。

【0008】ここで、音声オブジェクトデータは例えば、周知のCELP (Code Excited Linear Prediction) 符号化や、変換領域重み付けインターリーブベクトル量子化 (TWINVQ) 符号化等の高効率符号化が施されたデータであり、動画像オブジェクトデータは例えば、MPEG-4やH-263方式にて高効率符号化が施されたデータである。

【0009】また、オブジェクトディスクリプタは各オブジェクトに関する属性情報および再生に関する制御情報を含むデータである。

【0010】メモリ部104～106の各オブジェクトデータはそれぞれの復号部108～110へ入力される。復号部108～110において、上述のような高効率符号化された、動画像オブジェクトデータ、音声オブジェクトデータ、及びオブジェクトディスクリプタ等は復号される。ただし、メモリ部103に入力されたシーン記述情報のみは、シーン記述復号部107へ直接入力されて復号される。

【0011】尚、図1においては音声オブジェクト、動画像オブジェクト、オブジェクトディスクリプタについて夫々複数の互いに異なる種類のオブジェクトがMPEG-4ストリームに内に存在しても復号可能な装置を仮定しているため、メモリ部104～106や復号部108～110は音声用、動画像用、オブジェクトディスクリプタ用に夫々複数用意されているものとする。

【0012】そして、復号部108～110において夫々復号された音声オブジェクト、動画像オブジェクト、オブジェクトディスクリプタはシーン記述復号部107で復号されたシーン記述情報に基づいて、シーン合成部112にて合成／グラフィック処理が行われる。このようにして得られた最終的なデータ列はディスプレイやプリンタ装置といった出力機器113に供給されて可視化されることになる。ここで、音声あるいは動画像などのシーンを構成する個々のオブジェクトデータに対して、著作権などの保護のために再生を実行させたり、再生を停止させたりする制御が必要となる場合には、IPMP (Intellectual Property Management and Protection) シス

テムを用いて制御を行う。

【0013】IPMP制御部111は分離部102からのIPMPディスクリプタに基づき、必要に応じて制御ポイントにおいてストリームを遮断したり、復号部108～110にアクセスして、復号動作の停止を命令する。この“ディスクリプタ”とは、再生装置がデータを再生するときに必要となる制御情報等を記述するためのデータの集合であり、IPMPディスクリプタとはオブジェクトデータの再生制御に関わる情報を記述するために設けられたディスクリプタである。

【0014】このためIPMP制御部111が、IPMPディスクリプタ中のデータに基づいてデータの視聴の権利が無いと判断した場合には、該データが復号されなくなるので、再生が行われなくなる。このような制御を行うことで著作権を有するデータの保護を行う。

【0015】

【発明が解決しようとする課題】IPMP情報は、受信したデータの再生、制御に関わる重要な情報である。つまり悪意を持ったものが、受信データの視聴許可がないにもかかわらずこのIPMPデータに対して何らかのデータの改竄を行い、その結果不正にデータを視聴するといった可能性がある。

【0016】コンテンツの著作権者としては、不正防止を含む知的財産権保護システムがあれば安心してコンテンツを提供することができるが、該システムが不完全な場合にはコンテンツを提供することに躊躇することになる。

【0017】すなわちMPEG-4における知的財産権保護管理システムであるIPMPシステムのデータを保護・管理することで正当な加入者のみが受信データの視聴をすることができるようにすることはネットワークを使用したコンテンツ配信サービスのビジネスを立ち上げるため必要なものである。それにもかかわらず、IPMPデータを保護する手段は現在のところ講じられていない。

【0018】本発明はかかる問題点を鑑みなされたものであり、知的財産権保護管理システムを備えるマルチメディア符号化方式において、コンテンツ内の情報に対するセキュリティ機能を向上させたコンテンツ作成方法及び装置、コンテンツ再生方法及び装置、並びにコンピュータ可読記憶媒体を提供しようとするものである。

【0019】

【課題を解決するための手段】上記目的を達成するために、その一つの発明のコンテンツ作成方法／装置は、知的財産保護管理システムを備えるマルチメディア符号化方式のコンテンツ作成方法／装置であって、コンテンツ内の情報のオリジナル性を検証するための検証用データを含む知的財産保護管理情報を発生し、前記知的財産保護管理情報をコンテンツに、前記知的財産保護管理システムが使用するメッセージ形態にして埋め込むことを特徴とする。

【0020】また、その一つの発明のコンピュータ可読記憶媒体は、上記のコンテンツ作成方法を実行するプログラムが記憶されたことを特徴とする。

【0021】また、その一つの発明のコンテンツ再生方法／装置は、知的財産保護管理システムを備えるマルチメディア符号化方式のコンテンツ再生方法／装置であって、コンテンツ内の情報のオリジナル性を検証するための検証用データを含む知的財産保護管理情報が埋め込まれたコンテンツを入力する入力工程／手段と、前記コンテンツ内の知的財産保護管理情報を検出する検出工程／手段と、前記検出結果に基づいて前記コンテンツの再生動作を制御する制御工程／手段とを有することを特徴とする。

【0022】また、その一つの発明のコンピュータ可読記憶媒体は、上記のコンテンツ再生方法を実行するプログラムが記憶されたことを特徴とする。

【0023】

【発明の実施の形態】以下、本発明の実施例について、図面を参照して説明する。まず、送信装置と再生装置とからなるデータ配信システム及びデータの生成方法、データ構成に関して説明し、次に該データ配信システムにおける送信装置の動作の一例、再生装置の動作の一例についてそれぞれフロー図を基に説明する。初めに送信装置およびMPEG-4ストリームが生成されるまでの流れを説明する。

【0024】図2において、編集／入力部201に入力された動画データは動画データ符号化部202においてMPEG-4やH-263といった符号化方式により符号化されて動画データオブジェクトデータに変換され、音声データは音声データ符号化部205において符号化されて音声データオブジェクトデータに変換され、静止画データは静止画データ符号化部206においてJPEGといった方式により圧縮されて静止画データオブジェクトデータに変換され、文字データはテキストデータ符号化部207においてテキストデータオブジェクトデータに変換される。

【0025】また、再生装置にてこれらの各オブジェクトデータをどのように合成し、どのようなタイミングで再生するかを指定する情報であるシーン記述情報が必要になる。このシーン記述情報は、編集者が編集／入力部201で行う編集作業に基づいて生成される編集データがシーン記述情報符号化部204で処理されることで生成される。

【0026】さらに、再生装置において、これらの個々のオブジェクトデータに対して、知的財産権（著作権）を保護する目的で再生を実行させたり、再生を停止させたりするための制御情報であるIPMPディスクリプタが生成される。このIPMPディスクリプタは、編集者が編集／入力部201で行う編集作業に基づいて生成される許可データがIPMPディスクリプタ生成部203で処理されることで生成される。

・【0027】多重化部208では動画像オブジェクトデータ、音声オブジェクトデータ、静止画オブジェクトデータ、テキストオブジェクトデータ、IPMPディスクリプタ、シーン記述情報が多重化されてMPEG-4ストリームが生成される。

【0028】前記MPEG-4ストリームは図3に示すようにシーン記述情報301、動画像オブジェクトデータ303、静止画オブジェクトデータ304、音声オブジェクトデータ305、テキストオブジェクトデータ306、オブジェクトデータの制御情報であるオブジェクトディスクリプタ302で構成される。

【0029】また、オブジェクトディスクリプタ302の一構成要素としてIPMPディスクリプタ307が存在する。従ってIPMPディスクリプタ307はオブジェクトディスクリプタ302の一構成要素として送られる。

【0030】以下で具体的なIPMPディスクリプタの生成方法の一方法について説明する。本実施例では、編集者はIPMPシステムを用いて動画像データの視聴制御を行うものとする。従って、編集者は動画像データのどの部分に対してIPMPシステムによる視聴制限を行うかという入力作業を入力／編集部201にて行う。どんな単位で動画像データの視聴制御に関する指定を行うかに関して、本実施例ではフレームを指定の単位とするが、それに限るものではなく、所定データ量単位でも良い。

【0031】本実施例では動画像データを構成するフレームをカウントすることが必要になる。ここで、1フレームとはフレーム内部に含まれるデータのみで1枚の画像を構成することのできる単位である（動画像はいくつかの画像の集まりで構成されている）。

【0032】フレーム数のカウントは、動画像データのヘッダにある情報と前記動画像データのデータ量とから算出することができる。カウント終了後、入力／編集部201に接続されているディスプレイ201a上に、入力された動画像データを構成するフレームが1枚毎にフレーム番号と共に表示される。編集者はこのディスプレイ201aを見ながらどのフレームに対して視聴制限を行うかということを決定し、キーボード等の操作部201bにより入力／編集部201にその決定に基づいた視聴制限の情報を入力する。

【0033】視聴制限の情報を入力することで、編集／入力部201は図4に示すような許可データを生成する。

【0034】図4では、編集者が1フレームから100フレームまで連続、201フレームから300フレームまで連続、の視聴制限を行い、その他のフレームは視聴制限を行わないという設定を行った時に生成されるデータである。本実施例では全フレーム数は500フレームであり、視聴制限が行われるフレームの範囲にはフラグとして1が設定され、そうでないフレームには0が設定される。

【0035】前記許可データはIPMPディスクリプタ生成部203へ送られ、図5に示す実情報の領域506に格納される。

【0036】ここでIPMPディスクリプタの構造を図5に基づいて説明する。IPMPディスクリプタ307におけるタグ値501は該IPMPディスクリプタ307が開始することを示すデータであり、データ長502はIPMPディスクリプタ307のデータ長に関するデータが記述される。

【0037】IPMPディスクリプタID503はIPMPディスクリプタが複数存在した場合にそれぞれを区別するためのID情報であり、IPMPタイプ504は次のオプション領域にどのようなデータが存在するかを示すデータである。IPMPタイプ504の領域に格納された値が“0”の場合にはオプション領域505に実情報506が在り、IPMPタイプ504の領域に格納された値が“1”の場合にはオプション領域505にURL情報507が在ることをそれぞれ示す。

【0038】このように、IPMPデータはオブジェクトデータの視聴制限に関わる重要なデータである。従ってシステムを攻撃して不正にデータを視聴しようとする者は先ずこのIPMPディスクリプタを改竄することが予想される。

【0039】そこでIPMPシステムへの攻撃に対処するために、前記IPMPディスクリプタの正当性をチェックするためのデジタル署名データをIPMPディスクリプタの実情報のエリアに付加することとする。上記で説明したIPMPディスクリプタの構造はMPEG-4の規格上決まっているものであり、「MPEG-4規格準拠」を謳うためには上記の規格に従う必要がある。しかし、実情報のデータの記述方法には、現時点において規格上何の制限もない。従ってIPMPディスクリプタのデジタル署名データをIPMPディスクリプタの実情報のエリアに付加することは規格に反することではない。

【0040】ここでデジタル署名データについて説明する。デジタル署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認するためのものである。「電子署名及び認証業務に関する法律案」によるとデジタル署名（電子署名）の定義は「電磁的記録に記録することができる情報について行われる措置であって、次の要件に何れにも該当するものをいう。一、当該情報が当該措置を行った者の作成に関わるものであることを示すためのものであること二、当該情報について改変が行われていないかどうかを確認することができるものであること」となっている。

【0041】上記定義を満たすデジタル署名の一つは、公開鍵暗号とハッシュ関数とを用いることで実現できる。その方法を以下で説明する。初めに公開鍵暗号について説明する。公開鍵暗号は暗号鍵と復号鍵が異な

り、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。

【0042】公開鍵暗号の特徴としては、

(a)暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(b)各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

(c)送られてきた通信文の送信者が偽者でないこと及びその通信文が改竄されていないことを受信者が確認するための認証機能を実現できる。

が挙げられる。例えば、平文データ  $M$  に対して、公開の暗号鍵  $K_p$  を用いた暗号化操作を  $E(K_p, M)$  とし、秘密の復号鍵  $K_s$  を用いた復号操作を  $D(K_s, M)$  とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

(1) $K_p$  が与えられたとき、 $E(K_p, M)$  の計算は容易である。 $K_s$  が与えられたとき、 $D(K_s, M)$  の計算は容易である。

(2)もし  $K_s$  を知らないなら、 $K_p$  と  $E$  の計算手順と  $C = E(K_p, M)$  を知っていても、 $M$  を決定することは計算量の点で困難である。次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

(3)全ての平文データ  $M$  に対し、 $E(K_p, M)$  が定義でき、 $D(K_s, E(K_p, M)) = M$  が成立する。つまり、 $K_p$  は公開されているため誰もが  $E(K_p, M)$  を計算することができるが、 $D(K_s, E(K_p, M))$  を計算して  $M$  を得ることができるのは秘密鍵  $K_s$  を持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証が実現できる。

(4)すべての平文データ  $M$  に対し、 $D(K_s, M)$  が定義でき、 $E(K_p, D(K_s, M)) = M$  が成立する。つまり、 $D(K_s, M)$  を計算できるのは秘密鍵  $K_s$  を持っている本人のみであり、他の人が偽の秘密鍵  $K_s'$  を用いて  $D(K_s', M)$  を計算し  $K_s$  を持っている本人になりすましたとしても、 $E(K_p, D(K_s', M)) \neq M$  なので受信者は受けとった情報が不正なものであることを確認できる。また、 $D(K_s, M)$  が改竄されても  $E(K_p, D(K_s, M')) \neq M$  となり、受信者は受けとった情報が不正なものであることを確認できる。

【0043】上記の秘密通信と認証通信とを行うことができる代表例としてRSA暗号やR暗号やW暗号等が知られている。ここで、現在最も使用されているRSA暗号の暗号化、復号は次式で示される。

暗号化：暗号化鍵  $(e, n)$     暗号化変換  $C = M^e \pmod{n}$

復号：復号鍵  $(d, n)$     復号変換  $M = C^d \pmod{n}$

$n = p \cdot q$     ここで  $p, q$  は大きな異なる素数

上記の公開鍵暗号を用いた、データ正当性確認のためのデジタル署名データの生成および検証方法は以下のようになる。データの送信者は送信データ  $M$  に対して自身

が所有する秘密鍵  $K_s$  による演算  $D(K_s, M)$  を行い、デジタル署名データ  $s$  を生成する。そしてデジタル署名データ  $s$  と平文データ  $M$  とを受信者に送信する。

【0044】受信者は受け取ったデジタル署名データ  $s$  を送信者の公開鍵  $K_p$  による演算  $E(K_p, s)$  を行い、前記演算結果  $M'$  と受信データ  $M$  とを比較する。比較の結果  $M$  と  $M'$  とが一致した場合には、受信したデジタル署名データ  $s$  は送信者の秘密鍵  $K_s$  で演算処理されていることになる。

【0045】送信者の秘密鍵  $K_s$  は、送信者のみが知りうる情報であるので、①受信者は送信者が署名データを生成したこと、データが一致したことから②送信データ  $M$  が改竄されていないことを検証できる。公開鍵暗号は暗号化にも復号にもべき乗演算と剰余演算が必要であるので、共通鍵暗号と比較すると演算量が膨大なものとなり高速な処理は難しい。従って、送信データ  $M$  に対して公開鍵暗号の演算処理を行うのではなく、あらかじめ一定の大きさのデータに圧縮、前記圧縮されたデータに対して公開鍵暗号の演算処理を行うことが一般に行われている。この圧縮にハッシュ関数を用いる。このハッシュ関数  $H()$  は任意の長さの平文データ  $M$  に処理を行い、一定の長さの出力  $H(M) = h$  を出す機能を持つ。ここで、出力  $h$  を平文データ  $M$  のハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。ハッシュ関数に要求される性質として、一方向性と衝突耐性が要求される。一方向性とは  $h$  を与えた時、 $h = H(M)$  となる平文データ  $M$  の算出が計算量的に困難であることである。衝突耐性とは平文データ  $M$  を与えた時、 $H(M) = H(M')$  となる平文データ  $M' (M \neq M')$  の算出が計算量的に困難であること及び  $H(M) = H(M')$  かつ  $M \neq M'$  となる平文データ  $M, M'$  の算出が計算量的に困難であることである。ハッシュ関数としてはMD-2、MD-4、MD-5、SHA-1、RIPEMD-128、RIPEMD-160等が知られており、これらのアルゴリズムは一般に公開されている。公開鍵暗号に加えてこのハッシュ関数を用いた場合におけるデータ正当性確認のためのデジタル署名データの生成および検証は以下になる。平文データ  $M$  をハッシュ関数により圧縮して一定長の出力  $h$  を算出する演算を行う。次に、送信者の秘密鍵  $K_s$  で  $h$  を変換してデジタル署名データ  $s$  を作成する演算すなわち  $D(K_s, h) = s$  を行う。その後、前記デジタル署名データ  $s$  と平文データ  $M$  とを送信する。

【0046】一方、受信者は受信したデジタル署名データ  $s'$  を公開鍵  $K_p$  で変換する演算すなわち  $E(K_p, s') = h'$  と、受信した平文データ  $M'$  を発信者と同じハッシュ関数により圧縮して  $h''$  を算出する演算を行い、 $h'$  と  $h''$  が一致すれば受信したデータ  $M'$  を正当であると判断する。

【0047】平文データ  $M$  が送受信間で改竄された場合には  $E(K_p, s) = h'$  と、受信した平文データ  $M'$  を発信者と同じハッシュ関数により圧縮した  $h''$  が一致しないので

改竄を検出できる。ここで、平文データMの改竄に合わせてデジタル署名データsの改竄も行われてしまうと改竄の検出ができなくなる。しかし、これはhから平文データMを求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。

【0048】従って、前記デジタル署名データをIPMPディスクリプタ内に付加することで、MPEG-4データの伝送途中でIPMPディスクリプタ内のデータが改竄された場合には再生装置においてデジタル署名データをチェックすることで改竄を察知し、データの再生を停止することが可能になる。つまり、オブジェクトデータの著作権保護の強化につながる。

【0049】そこで、前記デジタル署名データから構成されるデータを“署名ディスクリプタ”という制御情報としてIPMPディスクリプタの実情報エリアに付加することとする。

【0050】以下で、署名ディスクリプタ及びデジタル署名データの生成について説明する。

【0051】最初に、署名ディスクリプタの構造の一例を図6に基づいて説明する。図6において、タグ値601には該署名ディスクリプタが開始することを示すデータであり、ディスクリプタ全体のデータ長602には前記署名ディスクリプタのデータ長に関するデータが記述される。

【0052】前記署名データ生成のためにどのハッシュ関数とどの公開鍵暗号アルゴリズムを使用したかを示す署名の種類603が次に記述される。署名データ長604には、署名データのデータ長に関するデータが記述される。署名データ605には、生成した署名データそのものが記述される。鍵データの種類606には、次のエリアに記述される鍵データの種類が記述される。鍵データ607には、再生装置で行う署名データ検証に使用するデータであり、公開鍵暗号方式によりデジタル署名データを生成した場合にはこのエリアには使用した秘密鍵Ksに対応する公開鍵Kpが記述される。この時、鍵データの種類606には公開鍵を示すデータが記述される。また、デジタル署名データ検証に必要となるデータ（鍵データ）をURLで公開して、再生装置において前記URLにアクセスしてから署名データ検証を行うような場合、鍵データの種類606にはURLを示すデータが記述され、鍵データ607に実際のURLアドレスが記述されることになる。

【0053】次に、デジタル署名データの生成について説明する。IPMPディスクリプタ生成部203は、IPMPディスクリプタの署名ディスクリプタを除く全てのデータ部のデジタル署名データを生成して署名データ605に格納する。つまり、本実施例の場合には、IPMPディスクリプタのタグ値、データ長、IPMPディスクリプタID、IPMPタイプ、許可情報 の全データDに対してハッシュ関数H( )による演算を行い、該演算結果のハッシュ値

$h = H(D)$ に対して送信装置が有する秘密鍵Ksにて演算を行いデジタル署名データ $S = D(Ks, h)$ を生成することになる。

【0054】次に、上述のように生成されたMPEG-4ストリームを再生するための再生装置の一例を図7を用いて説明する。

【0055】図7は、再生装置の構成を示すブロック図である。図7において、まずMPEG-4ストリームが入力されてから表示装置に表示されるまでの流れを説明する。

【0056】入力されたMPEG-4ストリームは、分離部701で動画像オブジェクトデータ、IPMPディスクリプタ、シーン記述情報、音声オブジェクトデータ、静止画オブジェクトデータ、テキストオブジェクトデータに分離され、それぞれの復号部702～707に入力される。この各復号部は内部にメモリを有しており、各オブジェクトデータは一旦メモリに格納されてから処理される。各復号部では、各オブジェクトデータのヘッダの中にある復号時間情報に従って各オブジェクトデータが復号されて、動画像データ、シーン記述情報、音声データ、静止画データ、文字データが生成される。

【0057】これらのデータは合成部708において、各オブジェクトデータのヘッダの中にある合成時間情報とシーン記述情報に従って合成されてディスプレイといった表示装置で表示されることになる。

【0058】次に、動画像オブジェクトデータの視聴制御およびデジタル署名データ検証について説明する。

【0059】IPMP制御部703は、送られたIPMPディスクリプタから許可データを抽出する。前記許可データは送信装置の編集／入力部で生成されたデータである。IPMP制御部703では、前記許可データに従って動画像復号部702へ制御を行う。本実施例の場合、図4に示したように1～100までのフレームには視聴制限がかかっているので、動画像復号部702に対して1～100までのフレームの復号データを合成部708に出力しないように制御を行う。従って、合成部708で動画像データを合成できないので動画像が表示されることはない。

【0060】これに対して101～200までのフレームには視聴が許可されているので、動画像復号部702に対して101～200までのフレームの復号データを合成部708に出力するように制御を行う。従って、合成部708で動画像データが合成されるので動画像が表示されることになる。

【0061】以下同様にIPMP制御部703は視聴が制限されているフレームのデータを合成部708に出力しないように、視聴が許可されているフレームのデータを合成部708に出力するように動画像復号部702に対して制御を行う。このようにして編集者の意図したように動画像データの視聴制御が可能になる。以下では再生装

置が行う、上記の制御動作の前に行うIPMPディスクリプタの検証動作について説明する。

【0062】IPMP制御部703はタグ値の値から、IPMPディスクリプタ内の署名ディスクリプタを識別する。そして前記署名ディスクリプタ中の署名データ $S'$ を抽出する。更に、送信装置において公開鍵暗号方式によりデジタル署名データを生成した場合には、使用した秘密鍵 $K_s$ に対応する公開鍵 $K_p$ が記述されている鍵データから検証に使用する公開鍵 $K_p$ を抽出し、上記抽出した署名データ $S'$ に前記公開鍵 $K_p$ で処理を行い $h' = E(K_p, S')$ を生成する。

【0063】また、検証に必要なデータ（鍵データ）をURLで公開してある場合には、鍵データにURLのアドレスが記述されているので前記URLにアクセスして検証に必要なデータを取得してから上記演算を行う。

【0064】一方でIPMPディスクリプタ内の署名ディスクリプタを除く全てのデータのハッシュ関数による演算を行う。つまり本実施例の場合には、IPMPディスクリプタのタグ値、データ長、IPMPディスクリプタID、IPMPタイプ、許可情報の全データ $D'$ に対してハッシュ関数 $H()$ による演算を行う。そして前記ハッシュ関数による演算結果 $h'' = H(D')$ と上記公開鍵 $K_p$ による署名データの演算処理結果 $h'$ を比較する。

【0065】上記比較結果、2つの演算結果が一致した場合（ $h' = h''$ ）には、IPMPディスクリプタは改竄されていないと判断できるので、許可情報に従って上記の視聴制御を行うこととなる。

【0066】一方、上記比較結果、2つの演算結果が一致していない場合には、IPMPディスクリプタに何らかの改竄がされたと考えられる。そこで、IPMP制御部703は、動画像復号部702に対して一切の復号動作を行わないように制御を行うと共に改竄が検出された旨のメッセージを画面上に表示するように合成部708に指示を行う。このようなメッセージを表示することで受信者は、再生が出来ない理由が契約していないからか、何らかのデータの改竄が行われたためなのかを知ることができる。

【0067】上記実施例では、署名の種類のデータから前記署名データ生成にどのようなハッシュ関数と公開鍵暗号方式が使用されたかを検出し、使用されたハッシュ関数と公開鍵暗号方式と同一の関数と方式で上記の演算を行うこととなる。上記方法によれば、再生制御に関して重要なデータであるIPMPデータにもしも改竄が行われた場合、前記改竄をチェックすることができるので悪意を持った者の攻撃からシステムを防御できる。従って正当な視聴の権利を持つ者のみがデータを視聴することが可能になり、コンテンツの著作権者は安心してコンテンツを提供することができるのでネットワークを使用したコンテンツ配信サービスのビジネスを立ち上げることができる。

【0068】以下では本発明の装置の動作、特に送信装置の処理の一例について図8のフローチャートを用いて説明する。

【0069】図8は、送信装置がMPEG-4ストリームの生成を行う際の処理を説明するためのフローチャートである。また、本実施例では公開鍵暗号方式によりデジタル署名データを生成するものとする。

【0070】図8において、ステップ801では、編集者がオブジェクトデータに対してIPMPシステムを用いて視聴制御を行うための入力となされるかどうか判断される。視聴制限をIPMPシステムで行うという入力された場合にはステップ802に進み、入力となされない場合にはステップ806に進む。次に、ステップ802では、入力された視聴制限のデータに基づいて許可データを生成し、ステップ803に進む。

【0071】ステップ803では、タグ値501にはIPMPディスクリプタの開始を示すデータを、IPMPディスクリプタID503には複数のIPMPディスクリプタを識別するためのシリアル番号を、IPMPタイプ504には次のオプション領域505には実情報が書き込まれるので”0”を、実情報506には上記で生成した許可情報を、データ長502には、IPMPディスクリプタのデータ長を、それぞれ書き込むことでIPMPディスクリプタを生成する（図5参照）。

【0072】次にステップ804では、検証のためのデータであるデジタル署名データ等で構成される署名ディスクリプタをIPMPディスクリプタ内に挿入するための入力となされるかどうか判断される。この入力もまた編集者が行うものである。署名ディスクリプタを挿入するという入力された場合には、ステップ805に進み、上記入力がされない場合にはステップ806に進む。ステップ805では、IPMPディスクリプタのタグ値、データ長、IPMPディスクリプタID、IPMPタイプ、許可情報の全データ $D$ に対してハッシュ関数 $H()$ による演算 $H(D) = h$ を行う。

【0073】前記演算結果のハッシュ値 $h$ に対して送信装置が有する秘密鍵 $K_s$ にて演算を行いデジタル署名データ $s = E(K_s, h)$ を生成し、該デジタル署名データを署名ディスクリプタの署名データ605に書き込む。

【0074】この時にタグ値601には署名ディスクリプタの開始を示すデータを、署名の種類603にはデジタル署名データ生成に使用されたハッシュ関数と公開鍵暗号のアルゴリズムの種類を示すデータを、署名データ長604には上記で生成したデジタル署名データ $s$ のデータ長を、鍵データの種類606には公開鍵を示すデータを、鍵データにはデジタル署名データ $s$ の生成に使用した秘密鍵 $K_s$ に対応する公開鍵 $K_p$ を、ディスクリプタのデータ長602にはこのディスクリプタ全体のデータ長を、それぞれ書き込む（図6参照）。

【0075】ここで、前記署名ディスクリプタをIPMPデ



ィスクリプタ中に挿入したことによってIPMPディ  
スクリプタのデータ長が変化することになるので、IPMPディ  
スクリプタのデータ長502に記述されているデータの更  
新を行う。次にステップ806では、動画像データ、音  
声データ、静止画データ、テキストデータ、シーン記述  
情報といった各データの符号化がそれぞれの符号化部  
にて行われ、ステップ807に進む。

【0076】ステップ807では、上記で生成された各  
オブジェクトデータ、ディスクリプタ（この中にIPMPデ  
ィスクリプタも含まれる）が多重化されてMPEG-4スト  
リームが生成される。

【0077】次にステップ808では、上記で生成され  
たMPEG-4ストリームが伝送路で、またはCD-ROMといっ  
た記録媒体にコピーされた後に再生装置に送られ、処理  
が終了する。

【0078】以下では本発明の装置の動作、特に再生装  
置の処理の一例について図9のフローチャートを用いて  
説明する。

【0079】図9は、上記の送信装置で生成され、再生  
装置が受信したMPEG-4ストリームの再生処理を説明す  
るためのフローチャートである。

【0080】図9においてステップ901では、送信装  
置で生成されたMPEG-4ストリームを伝送路から、また  
はCD-ROMといった記録媒体から受信する。

【0081】次にステップ902では、受信したMPEG-  
4ストリームを動画像データ、音声データ、静止画デー  
タ、テキストデータ、シーン記述情報、オブジェクトデ  
ィスクリプタといった各オブジェクトデータに分離し、  
ステップ903に進む。

【0082】ステップ903では、上記で分離されたオ  
ブジェクトディスクリプタの中にIPMPディスクリプタが  
存在するかどうかをチェックされる。前記チェックはオ  
ブジェクトディスクリプタの中にIPMPディスクリプタを  
示すタグ値が存在するかどうかで行われる。IPMPディ  
スクリプタが存在する場合にはステップ905に進み、存  
在しない場合にはステップ904に進む。

【0083】ステップ904では、どのオブジェクトデ  
ータにもIPMPシステムによる視聴制限が設定されてい  
ないことを意味するので各オブジェクトデータはそれぞ  
れの復号部で復号された後、出力機器に出力され処理が  
終了する。ステップ905では、IPMPディスクリプタの中  
に署名ディスクリプタが存在するかどうかをチェックす  
る。前記チェックはIPMPディスクリプタの中に署名デ  
ィスクリプタを示すタグ値が存在するかどうかで行われ  
る。署名ディスクリプタが存在する場合には、ステップ  
906に進み、存在しない場合にはステップ908に進  
む。

【0084】ステップ906では、署名の種類603に  
記述されているデータから検証に使用するハッシュ関数  
と公開鍵暗号アルゴリズムを識別する。次に署名データ

長604に記述されているデータに基づいて署名データ  
605に記述されている署名データ $s'$ を抽出する。次に  
鍵データ607から検証に使用する公開鍵 $K_p$ を抽出し、  
上記で抽出した署名データ $s'$ に該公開鍵 $K_p$ で演算処理を  
行い $h' = E(K_p, s')$ を生成する。該演算には上記で識別  
した公開鍵暗号アルゴリズムを使用する。

【0085】さらにIPMPディスクリプタ内の署名ディ  
スクリプタを除く全てのデータのハッシュ関数による演算  
を行う。つまりIPMPディスクリプタのタグ値、データ  
長、IPMPディスクリプタID、IPMPタイプ、許可情報の全  
データ $D'$ に対してハッシュ関数による演算を行う。前記  
ハッシュ演算にも上記で識別したハッシュ関数が使用さ  
れる。

【0086】そして、前記ハッシュ関数による演算結果  
 $h'$ と $H(D')$ と上記公開鍵 $K_p$ による署名データの演算処理  
結果 $h'$ を比較する。上記比較結果、2つの演算結果が一  
致した場合（ $h' = h''$ ）には、IPMPディスクリプタは改竄  
されていないと判断してステップ908に進む。

【0087】一方、上記比較結果、2つの演算結果が一  
致していない場合には、IPMPディスクリプタに何らかの  
改竄がされたと判断してステップ907に進む。ステッ  
プ907では、IPMPディスクリプタに改竄が検出された  
ので、一切の復号動作を行わないようにすると共に改竄  
が検出された旨のメッセージを画面上に表示し処理が終  
了する。

【0088】ステップ908では、IPMPディスクリプタ  
ID503に記述されている情報を確認してから、IPMPタ  
イプ504に記述されているデータからオプション領  
域505の記述されているデータが実情報であるか、UR  
L情報であるかを判断した後、オプション領域505  
のデータを抽出する。本実施例の場合は送信装置におい  
て許可データが実情報として記述されているので、許可  
データを抽出後に前記許可データに基づいて上記で記述  
したようにIPMPシステムによる制御が行われる。

【0089】本発明は一つの機器（例えば複写機、ファ  
クシミリ）からなる装置に適用しても、複数の機器（例  
えばホストコンピュータ、インタフェース機器、リー  
ダ、プリンタ等）から構成されるシステムに適用しても  
よい。また、前述した実施形態の機能を実現する様に各  
種のデバイスを動作させるために、該各種デバイスと接  
続された装置あるいはシステム内のコンピュータに、前  
記、実施形態を実現するためのソフトウェアのプログラ  
ムを供給し、そのシステムあるいは装置のコンピュータ  
(CPU, MPU)を格納させたプログラムに従って前記各種デ  
バイスを動作させることによって実施したものも本発明  
の範疇に含まれる。

【0090】またこの場合、前記ソフトウェアのプログ  
ラム自体が前述した実施形態の機能を実現することにな  
り、そのプログラムコード自体、及びそのプログラムコ  
ードをコンピュータに供給するための手段、例えばプロ

グラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを格納する記憶媒体としては例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、DVD-ROM、不揮発性のメモリカード等を用いることができる。

【0091】またコンピュータが、供給されたプログラムコードを実行することにより、前述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して前述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその拡張機能ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も本発明の実施の形態に含まれることは言うまでもない。

【0092】また、上記実施例では動画像データに対する知的財産権の保護管理について述べたが、動画像データに限るものではなく、音声データ、静止画像データ等に対しても同様な方法により知的財産権の保護管理を行うことができる。

【0093】

【発明の効果】本発明によれば、知的財産保護管理シス

テムを備えるマルチメディア符号化方式において、コンテンツの知的財産権（著作権）に対する保護・管理機能を向上させることができる。従って正当な視聴の権利を持つ者のみがデータを再現することが可能になり、コンテンツの知的財産権（例えば、著作権）者は安心してコンテンツを提供することができるのでネットワークを使用したコンテンツ配信サービスが現実的なものとなる。

【図面の簡単な説明】

【図1】本発明におけるMPEG-4再生装置の概略構成を示すブロック図である。

【図2】本発明における実施例の送信装置の概略構成を示すブロック図である。

【図3】本発明における実施例のMPEG4ストリームの構造を示す図である。

【図4】本発明における実施例の許可データの構造を示す図である。

【図5】本発明における実施例のIPMPディスクリプタの構造を示す図である。

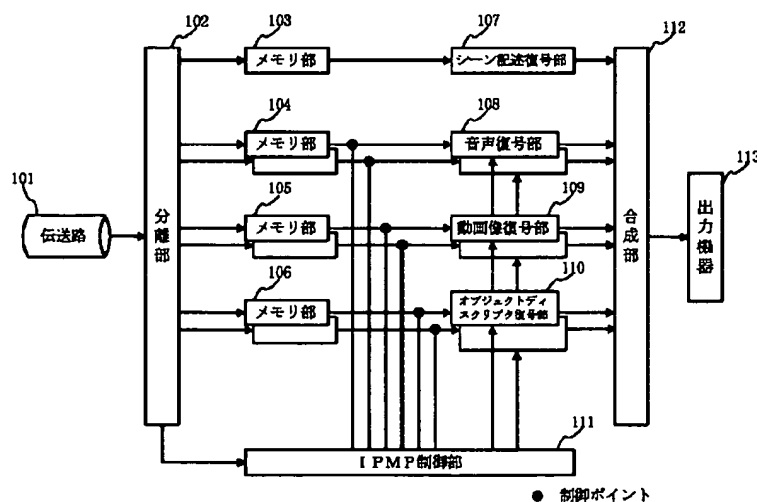
【図6】本発明における実施例の署名ディスクリプタの構造を示す図である。

【図7】本発明における実施例の再生装置の概略構成を示すブロック図である。

【図8】本発明における実施例の送信装置の動作を説明するためのフローチャートである。

【図9】本発明における実施例の再生装置の動作を説明するためのフローチャートである。

【図1】

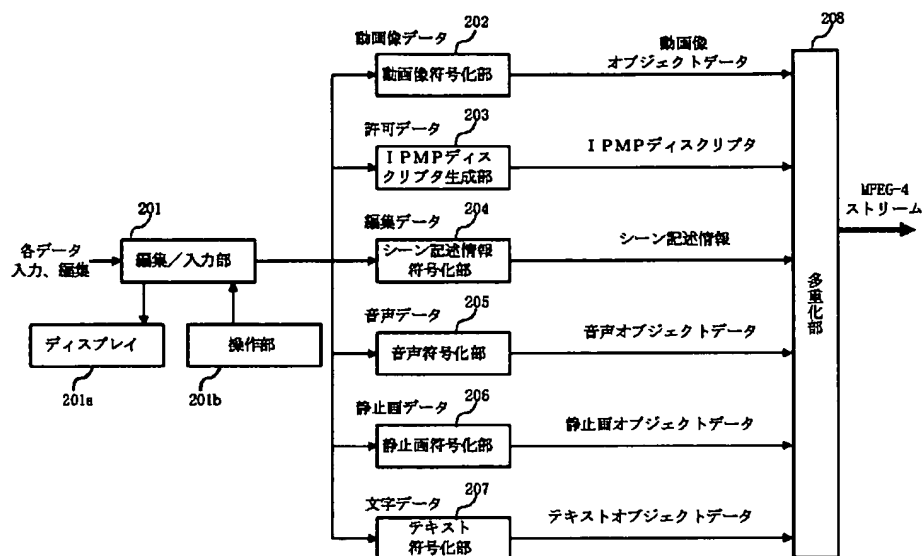


【図4】

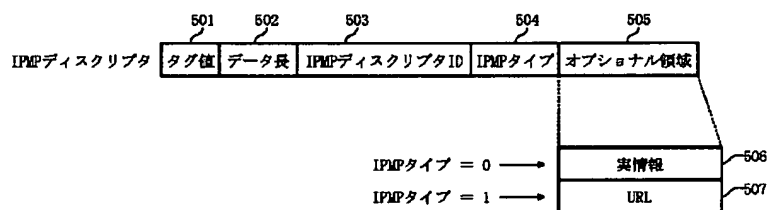
フレーム	フラグ
1~100	1
101~200	0
201~300	1
301~500	0

0: 視聴許可  
1: 視聴不許可

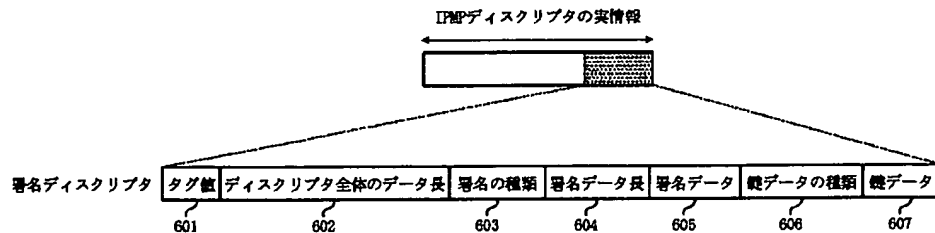
【図2】

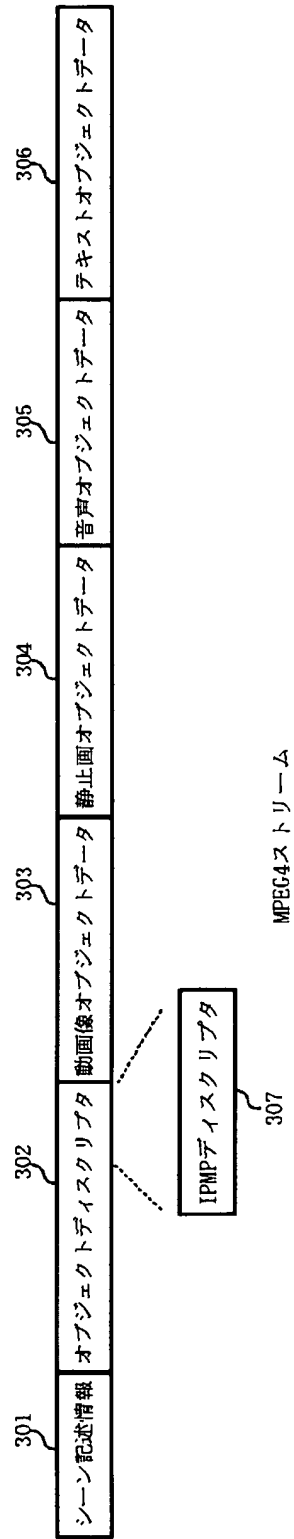


【図5】



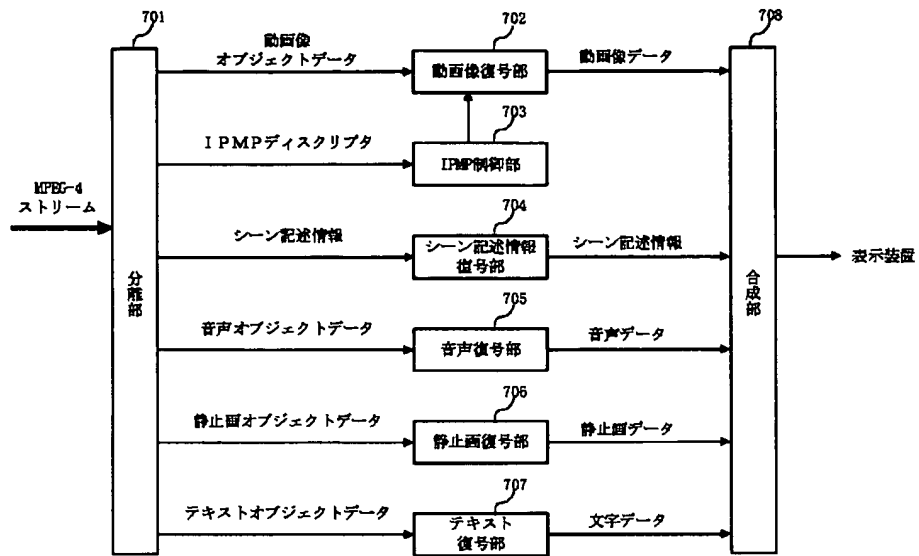
【図6】



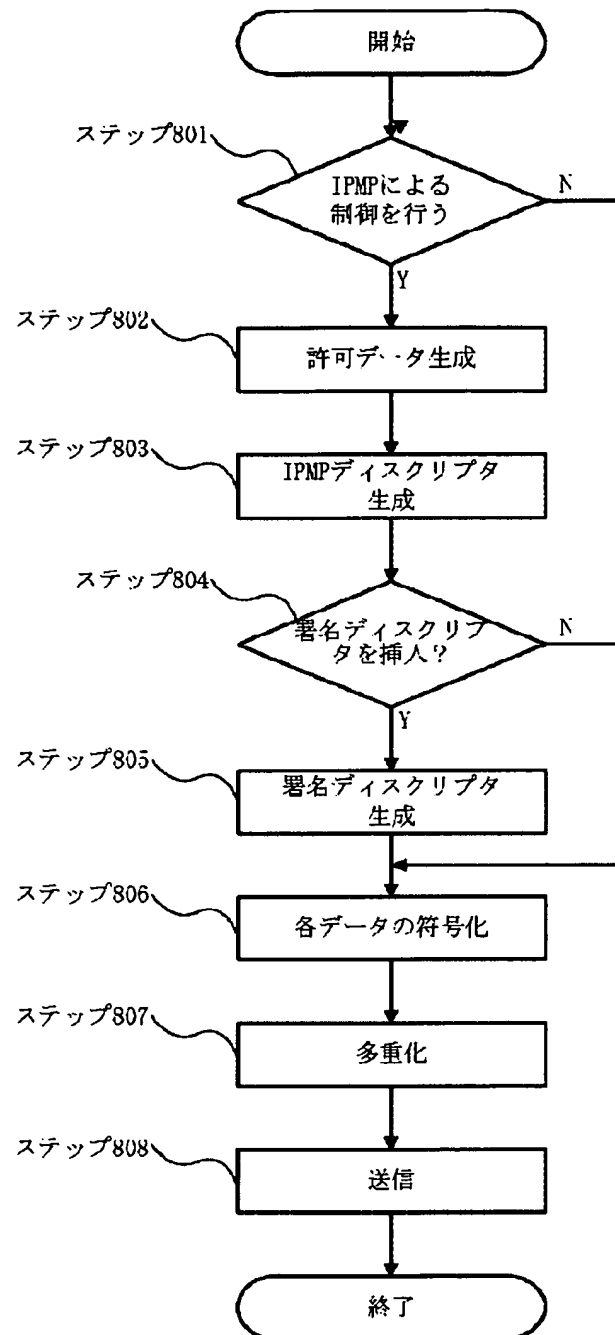


【図3】

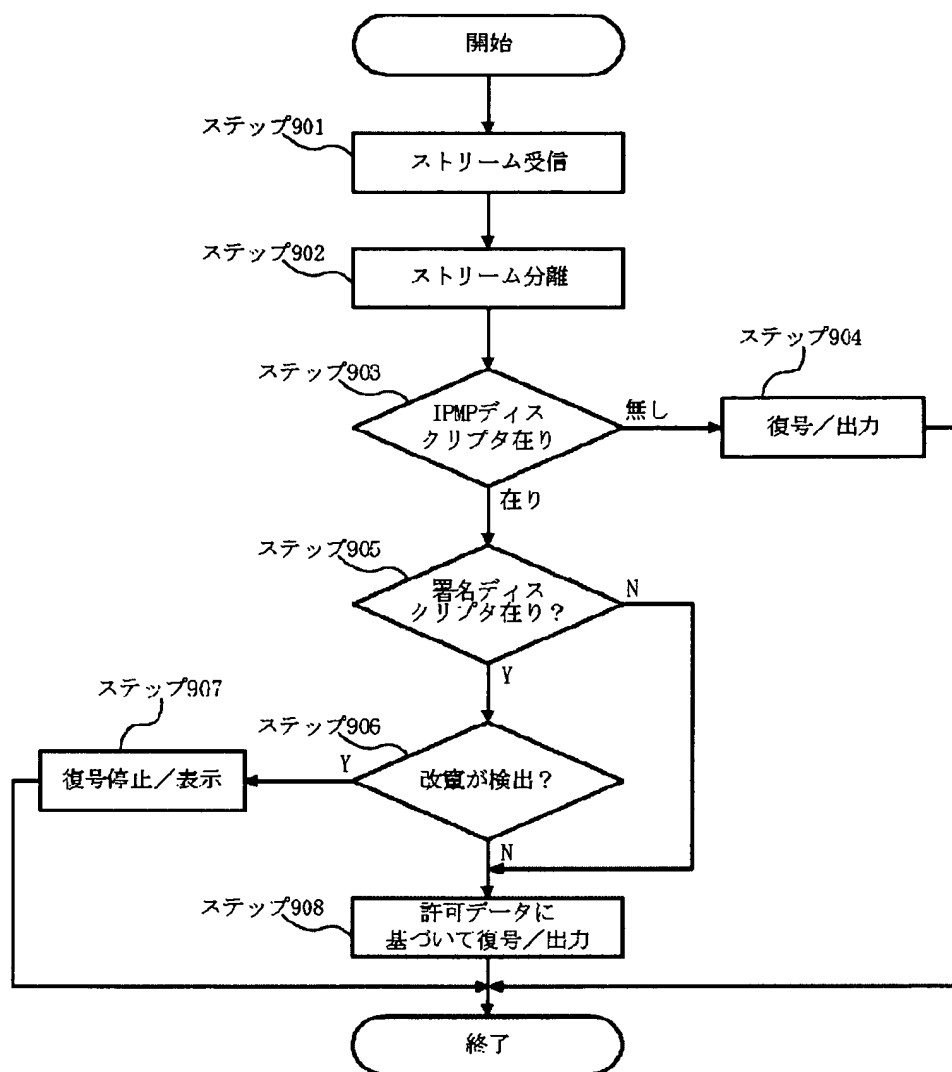
【図 7】



【図8】



【図9】



フロントページの続き

(72)発明者 須賀 祐治  
東京都大田区下丸子3丁目30番2号キャノ  
ン株式会社内

Fターム(参考) 5C059 KK43 MA00 MB22 MB29 RB18  
RC19 RC32 RC33 RC34 RC35  
SS20 UA02  
5C063 AC01 CA11 CA23 CA36 CA40  
DA07  
5C076 AA14 BA03 BA04 BA06  
5J104 AA09 LA03 LA05 LA06 NA12